AI Makes Phishing Smarter

Some phishing attacks are now AI-Driven. They are more convincing, faster, and harder to spot than traditional techniques.

DON'T TAKE THE BAIT!

They Mimic Tone and Grammar Perfectly

The new techniques see cybercriminals using AI to craft flawless emails that look pretty much completely authentic. This can make it much harder to spot errors or suspicious language.

Phishing Kits (PHaaS) Make Attacks Easy

Phishing-as-a-Service (PHaaS) platforms sell "phishing kits" that enable cybercriminals, even non-technical ones, to launch sophisticated and convincing phishing campaigns.

Beware of QR Codes and MFA Bypass Tricks

Scammers may embed malicious QR codes in emails or other documents, like PDFs, in an attempt to trck users into scanning them and bypassing any multi-factor authentication that may be set up.

Hover Over Links; Check Sender Details

Always verify things in any email before you click! Inspect URLs for links and confirm that the sender's email address and other information are right before you click or download any attachments.

Enable Multi-Factor Authentication and Use It

As usual, multi-factor authentication is a must. Always use it when available and avoid approving any unexpected login, or other requests, that pop up to prevent MFA fatigue attacks.

Report Suspicous Emails Immediately

If the messsage is in your personal email, mark as spam, but if you get one at work: forward or flag any emails to your security team. Quick reporting leads to quicker awareness and mitigation.